Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

Melindungi Peranti Mudah Alih Anda

Pengenalan

Peranti mudah alih anda merupakan cara terbaik dan mudah untuk berhubung dengan rakan-rakan, membeli-belah atau perbankan dalam talian, menonton filem, bermain dan melakukan pelbagai lagi aktiviti. Memandangkan peranti anda adalah sebahagian daripada perkara penting dalam hidup, berikut adalah beberapa langkah mudah untuk memastikan peranti dan anda sentiasa selamat.

Menjamin Peranti Anda

Ianya mungkin akan memeranjatkan tetapi risiko terbesar kepada peranti mudah alih anda bukanlah penggodam, tetapi anda sendiri. Kebarangkalian untuk kehilangan atau lupa peranti mudah alih anda berbandingianya digodam adalah lebih tinggi. Perkara pertama yang perlu dilakukan demi melindungi peranti anda adalah dengan membolehkan kunci automatik pada skrin, atau sering dipanggil kunci skrin. Ini bermakna setiap kali mahu menggunakan peranti anda perlu membuka kunci skrin dahulu, seperti menggunakan kod laluan yang kukuh atau cap jari anda. Jika peranti anda hilang atau dicuri ini membantu supaya tiada sesiapa dapat mencapainya. Sebagai tambahan, berikut adalah beberapa lagi langkah yang dapat membantu melindungi peranti anda:

Kemas kini

Bolehkan kemas kini automatik pada peranti anda supaya ia sentiasa menggunakan sistem operasi dan aplikasi terkini. Penyerang sentiasa mencari kelemahan terkini dalam perisian, dan vendor akan sentiasa mengeluarkan kemas kini dan tampalan untuk membaikinya. Dengan menggunakan sistem operasi dan aplikasi mudah alih terkini anda menjadikannya lebih sukar untuk sesiapa menggodam peranti tersebut.

Penjejakan

Pasang atau bolehkan perisian untuk menjejak peranti mudah alih anda melalui Internet. Dengan cara ini jika peranti dicuri, anda boleh bersambung dengannya melalui Internet dan dapatkan lokasinya, ataupun dalam kes terburuk anda boleh memadam semua maklumat di dalamnya.

Aplikasi Dipercayai

Hanya muat turun aplikasi yang anda perlukan dan daripada sumber yang dipercayai. Untuk iPad atau iPhone ini bermakna muat turun aplikasi dari Apple App Store. Untuk Android muat turun dari Google Play dan untuk tablet Amazon gunakan Amazon App Store. Walaupun anda masih boleh muat turun aplikasi dari laman lain, ia tidak disemak dan kebarangkalian untuk dijangkiti lebih tinggi. Sebelum memuat turun, semak jika aplikasi tersebut mempunyai banyak

ulasan positif dan ianya di kemas kini secara aktif oleh vendor. Jauhi aplikasi yang baru, aplikasi yang mempunyai ulasan yang sedikit atau jarang dikemas kini. Akhir sekali, tidak kira dari mana datangnya aplikasi anda, apabila tidak lagi menggunakannya atau jarang menggunakan aplikasi tersebut kami mencadangkan supaya anda memadamnya dari peranti.

Pilihan Privasi

Apabila memasang aplikasi baru, pastikan anda mengkaji semula pilihan privasi. Sebagai contoh, adakah aplikasi yang baru dimuat turun perlu mendapat capaian kepada semua rakan-rakan dalam maklumat kenalan? Kami juga menyarankan supaya anda melumpuhkan jejak lokasi untuk kesemuanya, dan membolehkan lokasi jika anda rasa aplikasi tersebut perlu menggunakannya. Jika tidak berasa selesa dengan keperluan kebenaran sesuatu aplikasi, cari aplikasi lain yang memenuhi kehendak anda. Sebagai tambahan, periksa kebenaran secara berkala untuk memastikan ia tidak bertukar.

Sandar

Sentiasa sandar maklumat anda. Untuk peranti mudah alih kebanyakan maklumat selalunya telah di sandar secara automatik, seperti gambar dan mesej anda. Walaubagaimanapun, sandar turut menyimpan tatarajah, aplikasi dan maklumat peranti yang lain, menjadikannya lebih mudah untuk memulihkan peranti yang hilang atau peralihan kepada peranti baru.

Kerja

semasa bekerja, sentiasa lebih waspada dan jangan sesekali mengambil gambar atau video yang mungkin boleh termasuk maklumat sensitif, seperti gambar papan putih atau skrin komputer.

Peranti mudah alih anda adalah suatu alat yang berkuasa, sesuatu yang digunakan dan dimanfaatkan. Dengan hanya mengikuti beberapa langkah ini anda mampu menjamin peranti dan anda untuk jangka masa yang lama.

Penterjemahan oleh SNSC.

Pusat Keselamatan Rangkaian SKMM (SKMM Network Security Centre- SNSC) beroperasi di bawah Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dengan matlamat menjamin keselamatan maklumat, kebolehpercayaan dan keutuhan rangkaian di Malaysia. Laman Web: http://snsc.skmm.gov.my/.

Sumber

Passphrases:	https://www.sans.org/u/A3E
Backup/Recovery:	https://www.sans.org/u/A3z
Disposing of Your Mobile Device:	https://www.sans.org/u/A3u
Securely Using Mobile Apps:	https://www.sans.org/u/A3p
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

lesen